The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
07/03/2020

SUBJECT:
Multiple Vulnerabilities in Cisco Products Could Allow for Administrator Privileges

OVERVIEW:
Multiple vulnerabilities have been discovered in Cisco products, the most severe of which could allow for an attacker gaining administrator privileges. Cisco is a vendor for IT, networking and cybersecurity solutions. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining administrator privileges. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Cisco AnyConnect Secure Mobility Client for Mac OS releases earlier than 4.9.00086
- Cisco Digital Network Architecture Center releases earlier than 1.2.10
- Cisco Identity Services Engine releases earlier than 2.6 Patch 7
- Cisco 250 Series Smart Switches
- Cisco 350 Series Managed Switches
- Cisco 350X Series Stackable Managed Switches
- Cisco 550X Series Stackable Managed Switches
- Cisco Small Business 200 Series Smart Switches
- Cisco Small Business 300 Series Managed Switches
- Cisco Small Business 500 Series Stackable Managed Switches
- Cisco Small Business RV042 and RV042G Routers firmware releases earlier than Release 4.2.3.14
- Cisco Unified Communications Manager
- Cisco Unified Communications Manager Session Management Edition
- Cisco Unified Communications Manager IM and Presence Service
- Cisco Unity Connection
- Cisco Unified Customer Voice Portal releases 12.5(1) and earlier

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Cisco Products, the most severe of which could result in an attacker gaining administrator privileges. These vulnerabilities can be exploited when maliciously crafted packets are sent to the vulnerable device. Details of the vulnerabilities are as follows:

- A vulnerability in session management for the web-based interface of Cisco Small Business Smart and Managed Switches could allow an unauthenticated, remote attacker to defeat authentication protections and gain unauthorized access to the management interface. (CVE-2020-3297)
- A vulnerability in the web-based management interface of Cisco Small Business RV042 Dual WAN VPN Routers and Cisco Small Business RV042G Dual Gigabit WAN VPN Routers could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. (CVE-2020-3431)
- Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker with administrative credentials to conduct a cross-site scripting (XSS) attack against a user of the interface. (CVE-2020-3340)
- A vulnerability in Cisco Digital Network Architecture (DNA) Center could allow an authenticated, remote attacker to view sensitive information in clear text. (CVE-2020-3391)
- A vulnerability in the Java Remote Method Invocation (RMI) interface of Cisco Unified Customer Voice Portal (CVP) could allow an unauthenticated, remote attacker to access sensitive information on an affected device. (CVE-2020-3402)
- A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. (CVE-2020-3420)
- A vulnerability in the web-based management interface of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM & Presence Service, and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. (CVE-2020-3282)
- A vulnerability in the uninstaller component of Cisco AnyConnect Secure Mobility Client for Mac OS could allow an authenticated, local attacker to corrupt the content of any file in the filesystem. (CVE-2020-3432)

Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining administrator privileges. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches or appropriate mitigations provided by Cisco to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack.
- Remind all users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding threats posed by hypertext links contained in emails or attachments especially from untrusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Cisco:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbswitch-session-JZAS5jnY
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sa-rv-routers-xss-K7Z5U6q3
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mlt-ise-strd-xss-nqFhTtx7
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-info-disc-6xsCyDYy
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cvp-info-dislosure-NZBEwj9V
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-bLZw4Ctq
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-cuc-imp-xss-OWuSYAp
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-mac-dos-36s2y3Lv

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3282
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3297
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3340
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3391
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3402
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3420
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3431
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3432